A US PAYMENTS FORUM WHITE PAPER

Connected Car and Contextual Payments

Version 1.0

Publication Date: May 2024

U.S. Payments Forum
544 Hillside Road
Redwood City, CA 94062

www.uspaymentsforum.org

About the U.S. Payments Forum

The U.S. Payments Forum is a cross-industry body that brings stakeholders together on neutral ground to enable efficient, timely and effective implementation of emerging and existing payment technologies. This is achieved through education, guidance and alternative paths to adoption. The Forum is the only non-profit organization whose membership includes the whole payments ecosystem, ensuring that all stakeholders have the opportunity to coordinate, cooperate on and have a voice in the future of the U.S. payments industry. The organization operates within the Secure Technology Alliance, an association that encompasses all aspects of secure digital technologies.

Table of Contents

Executive Summary

The convergence of automotive technology and digital payments has given rise to a transformative concept: the connected car and contextual payments ecosystem. This U.S. Payments Forum white paper delves into the intersection of these two domains, exploring the potential, challenges, and considerations for implementations.

In recent years, the automotive industry has witnessed a rapid evolution driven by connectivity, data analytics, and automation. The connected car, once a concept limited to infotainment, has evolved into a hub of sophisticated sensors, telematics, and communication channels. This evolution opens up avenues for safer, more efficient payments experiences, vehicle-to-vehicle communication, and integration with smart city infrastructure.

At the same time, the world of payments has been undergoing a digital transformation. Mobile wallets, touchless payments, and seamless online transactions have become the norm. Contextual payments, a novel concept, leverage real-time data and situational awareness to facilitate frictionless transactions. When applied to connected cars, contextual payments enable many use cases, from in-car purchases (e.g., fuel, tolls, parking) to personalized services (e.g., entertainment subscriptions, food delivery) that enhance the driving experience.

However, this convergence also presents challenges that must be addressed. Security and privacy are paramount, as the exchange of sensitive financial information within a vehicle's digital ecosystem raises concerns about data breaches and unauthorized access. Interoperability standards are crucial to ensure seamless collaboration among automakers, payment providers, and technology developers.

The benefits, nonetheless, are substantial. For consumers, the connected car and contextual payments integration offers convenience, time savings, and personalized experiences. For businesses, new revenue streams, data-driven insights, and opportunities for customer engagement are possible.

This white paper provides an analysis of the synergy between the connected car and contextual payments. It explores real-world examples and equips stakeholders across industries with the knowledge needed to navigate this evolving landscape successfully. At publication, new use cases are emerging into the marketplace that are not covered by this white paper.

1. Introduction

As the mobile and touchless payments market has grown, new, integrated user experiences are extending to connected cars to provide a contextual and seamless digital experience, enabling the driver to pay for gas, parking, and tolls, or order food through their vehicle's connected services. This paper's objectives are to inform merchants, original equipment manufacturers (OEMs), and other stakeholder groups about the topic of connected cars with an emphasis on contextual payments.

Readers are encouraged to reference other Mobile and Touchless Payments Working Committee resources, including:

- Mobile and Contactless Payments Requirements and Interactions white paper
- Mobile and Contactless Payments Glossary
- Mobile Payments Standards Glossary
- QR Codes FAQ

1.1 What Is Meant by Connected Car?

The connected car is a vehicle instrument connecting drivers to the digital world through connectivity (e.g., Wi-Fi, cellular, Bluetooth) and remote, over-the-air configuration of the vehicle. The way a car interacts with its environment—from parking meters to electric vehicle (EV) charging stations—continues to evolve. Through this connectivity, new payment experiences take the form of seamless and machine-to-machine-initiated payments. The industry continues to see more implementations that leverage connectivity with vehicles and car-centric experiences like contextual payments. In addition, digital services, such as purchasing entertainment directly through the vehicle's infotainment system, continue to grow. As more vehicles become connected and autonomous, the driver's experience will continue to evolve, and the user experience will be much different than today's. As devices get more connected to the internet and to each other, consumers will want and expect more and better experiences and ease of payment options.

1.2 What Are Contextual Payments?

Contextual payments are payments that occur without the need for the customer to produce a payment instrument or engage in a specific payment action. No direct interaction takes place between the customer and merchant at the time of payment. The payment occurs in the background, initiated by payment processing logic assessing the circumstances of the situation. Data, derived from geolocation, computer vision, biometrics, and/or sensors and computer logic of any kind, is used to make decisions as to when and how much to charge a customer, as well as what payment instrument to use.

A ride-sharing app is a common example of contextual payments. The customer has pre-enrolled a payment instrument and therefore does not need to produce a payment instrument as they would when completing a taxi ride. Instead, they exit the vehicle, and the payment occurs in the background. Another common example is an automated tolling system. Instead of providing cash or electronic payment to an attendant or machine, the toll is billed in the background based on a combination of geolocation, license-plate scanning, and, in the case of variable-priced toll roads, dynamic pricing decisions.

Payment occurs in the background and the customer has pre-approved the payment without using their physical card. Contextual payments leverage stored credentials with merchants or in-app purchases (where the consumer already stored their payment credentials).

1.3 Form Factors

In the context of the connected car, "form factors" typically refer to the physical shape, size, and design of the devices and components used to enable connectivity and other digital features in vehicles. A variety of components can be included, such as the infotainment system display, the human-machine interface (HMI) control panel, sensors, cameras, and connectivity modules.

With the increasing popularity of smartphone integration technologies such as Apple® CarPlay® and Android Auto™, mobile phones have become an important interface for drivers to access and control various features of their connected vehicles.

Examples of specific form factors in a connected car include:

- **In-dash displays**. Large screens are now integrated into the dashboard of the car and display information such as navigation directions, media playback, and vehicle diagnostics. They can also provide a mirror-like display of the driver's smartphone screen through technologies such as Apple CarPlay and Android Auto.
- **Cameras and sensors**. These devices are often used in advanced driver assistance systems (ADAS) to enable features such as adaptive cruise control, lane departure warnings, and automated parking. Some car models also include cameras that provide a 360-degree view of the vehicle's surroundings, which can be accessed through the car's in-dash display or a companion smartphone app.
- **Mobile phones and apps**. Mobile phones are an important form factor in the connected car, as they enable drivers to interact with their vehicles in a convenient and seamless way, from both inside and outside the car. Drivers can use their phones for a large variety of use cases.

Overall, form factors play an important role in the user experience with connected cars, as they determine how drivers and passengers interact with the technology and how seamlessly it integrates into the overall design of the vehicle.

1.4 Outbound Payments

An outbound payment in the context of this white paper is one that is initiated from the connected car to an external source. For example, a connected car could make a payment to a gas station for fuel or to a parking garage for parking fees.

Outbound and inbound payments refer to the flow of payments between the car and external sources, such as a driver's bank account or a merchant. This paper focuses on outbound payments. For example, a contextual outbound payment could be an outbound payment initiated by the driver or the car to pay for a specific service or product. By leveraging contextual information, outbound payments in connected cars can be made more convenient, personalized, and proactive. This enables a smoother and more frictionless payment experience for vehicle occupants, reducing the need for manual transactions and enhancing overall convenience.

1.5 Data Monetization

The evolution of a traditional vehicle to a connected car has cast new light on the growing role and value of data in the connected, contextual payments ecosystem. Every data touchpoint along the connection comes with its own potential to deliver seamless in-vehicle experiences and application possibilities for both consumer-to-business (C2B) and business-to-business (B2B) uses. Automotive OEMs are at the center of this change and find themselves entrusted with a new, unfamiliar role in the payments infrastructure.

At present, the industry does not have a unified approach for a common payment architecture that offers seamless integration into vehicles in order to achieve broad merchant acceptance and drive user adoption. The absence of standards has spawned proprietary approaches and incompatible payment solutions that obfuscate and compound concerns about data privacy, security, portability, and interoperability across the different industry players (including OEMs, merchants, processors, and financial institutions).

The driving forces that enabled the connected vehicle include a growing base of embedded and connected cellular-vehicle-to-everything (C-V2X) capabilities in vehicles, and the proliferation of in-vehicle communications through 5G cellular, Wi-Fi 6, and other low-power, wide-area networks. In addition, the declining costs of embedded and tethered hardware solutions and of communications made large-scale deployments commercially viable. The convergence of these technologies has extended mobile and touchless payments beyond the realm of phones and physical devices to native capabilities in the connected vehicle.

Automotive OEMs recognize the opportunities and threats that come with the new role of the vehicle as a payment instrument that enables seamless connected commerce for both C2B and B2B. Thrust into the center of the newfound payment opportunity, automotive OEMs are approaching this uncharted territory cautiously. The traditional automotive OEM business of producing hardware is increasingly melded with software and the ability to leverage data. The future of connected vehicles is no longer about making better cars, but rather smarter ones powered by software and real-time data.

The role of data as a strategic asset has attracted emerging players that are eager to monetize the opportunity. This new market has attracted entrants who are eager to establish computing platforms to power the connected vehicle and the payment capabilities within. The industry has also witnessed the emergence of new downstream data aggregators who repurpose and remarket data that can be used in a variety of value-added products and services that enhance the driver's experience and improve fleet management.

The road to achieving seamless contextual payment has many hurdles to overcome. Automotive OEMs know that they cannot succeed on their own. They also recognize potential concerns associated with reliance on proprietary solutions. Collaboration and partnership with other OEMs, standards organizations, governments, and industry players is essential to achieving a ubiquitous, contextual payment experience.

1.6 Infrastructure and Architecture

Connected car apps use wireless technology to perform their functions. Cellular networks (e.g., 5G, 4G) and Wi-Fi are examples of wireless technologies. They provide broad connectivity options and enable devices to connect to networks or the internet wirelessly over large distances. They are designed for high-speed data transmission, internet access, and interconnectivity between devices and networks.

Last-mile connectivity refers to the physical infrastructure and technologies between the internet service provider's network backbone and an end-user such as a merchant. This connectivity bridges the gap between the digital payment system and the point of sale or the recipient of the payment notification. Robust last-mile connectivity is important for enabling seamless and secure payment transactions in the physical world, particularly for use cases that require near-instant responsiveness between a merchant's physical location and a connected car, such as exiting a parking garage or enabling a fuel dispenser.

A managed network service provider (MNSP) is typically employed to design, implement, monitor, and scale last-mile connectivity requirements. They can also establish redundancy measures to ensure backup connectivity and avoid service outages.

Figure 1 illustrates the transaction process for a connected car.

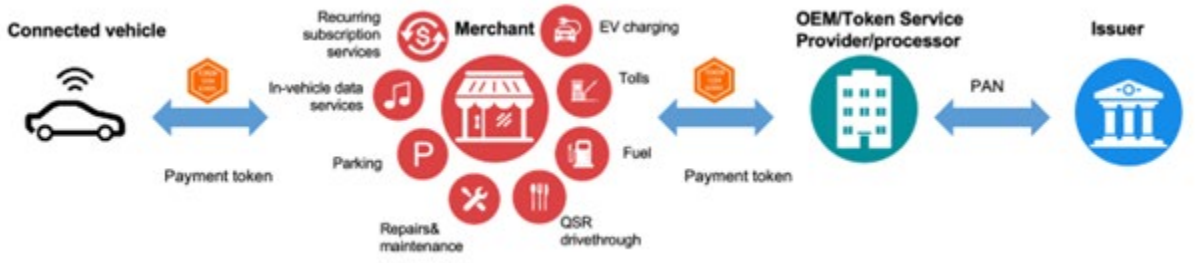

Figure 1. Connected Vehicle Transaction Flow[1]

[1] Note: images used in this white paper are for illustrative purposes only.

2. Considerations for Connected Car and Contextual Payments

2.1 Card-Not-Present and Card Present Transactions

Most implementations of connected car and contextual payments are considered card-not-present (CNP) transactions because they use technologies, such as an integrated in-app, digital wallet, or card-on-file solution, within the car system. As CNP transactions, the individual network operating rules and policies are applicable, such as security, fraud liability, chargebacks, and dispute rules.

Within the payments industry, various business rules, requirements and policies (e.g. those regarding security, fraud liability, chargebacks, dispute resolution, and other matters) may be set by applicable stakeholders (such as individual payment networks), and may depend on whether the transaction is deemed to be a card present (CP) transaction, or a card-not-present (CNP) transaction.

While card Present transactions are possible via embedded Secure Element or if vehicle is leveraging solutions using NFC chips in the vehicle's built-in screen or other SoftPOS/Tap to Screen solution, using NFC chips in the vehicle's built-in screen or other SoftPOS/Tap to Screen solution, comes with additional cost on both OEMs and merchants to accommodate for such new channel of payment. Contextual payments for connected cars are mainly considered as CNP transactions because most connected car use cases do not (or should not) relay on physical card presents at the time of purchase, instead leveraging technologies such as integrated in-app, digital wallets or card-on-file solutions within the car system.

Although a detailed discussion is beyond the scope of this paper, automotive OEMs, merchants, service providers and others considering connected cars and contextual payments are encouraged to be familiar with such business rules, requirements and policies and any associated business impacts.

2.2 Payment Tokenization

The basic benefit of contextual payment is delivering a seamless transaction experience that requires minimal or no user engagement and no physical payment instrument. A contextual payment transaction flows from the cardholder to the merchant to the financial institution and must securely pass through a variety of touchless channels and systems. A secure token replaces the physical payment instrument in this flow.

A token is a digital substitute for a physical card or payment account number that contains no meaningful sensitive data of exploitable value. The token contains reference information that maps back to the sensitive payment data that is managed through a tokenization system or token service provider (TSP). The use of application programming interfaces (APIs) enables different systems to securely communicate with each other and facilitate this seamless flow and handling of the token throughout the transaction.

The key benefits of tokenization for merchants include:

- Facilitate secure payment data sharing by replacing sensitive card information with a token that has no value without access to the encryption key used to generate it.
- Simplified data management by enabling data to be stored and transmitted more efficiently and securely.

- Reduced handling of actual payment data resulting in reduced payment cost and Payment Card Industry Data Security Standard (PCI DSS) scope and time spent on compliance.

Tokenization also provides benefits to cardholders, especially in improved security and convenience. These benefits play a role in defining the requirements and expectations for how contextual payments can work for the connected vehicle. The growing number of connected vehicle opportunities are expected to attract new competing payment tokens vying for a share of the digital wallet. Financial institutions' real-time payments solutions are examples of emerging digital wallets that has the potential to shape the future payment landscape due to its real-time payment capabilities.

Figure 2 illustrates the enrollment process for a connected car.

Figure 2. Payment Enrollment and Token Provisioning Flow

For the payment experience to be seamless, token interoperability across the different payment platforms and ubiquitous merchant acceptance are among the most critical goals to achieve. Automotive OEMs will need to determine how tokens can be provisioned, stored, managed, used, and accepted across the range of contextual payments use cases. The connected vehicle offers new payment revenue opportunities that do not currently exist. An important consideration includes whether to embrace existing payment tokenization processes or create new processes. The direction that automotive OEMs take will set precedence for the future of contextual payments as the era of autonomous vehicles arrives.

2.3 Alternate Payment Rails

Alternate payments rails from financial institutions have the potential to alter the contextual payment ecosystem. Currently consisting of person-to-person (P2P) transfers, real-time payments (RTP), and recently FedNow, these networks offer consumers and businesses alternative payment choices that can potentially transform the future of payments in connected vehicles. Widely regarded as the new cash, the key benefits to consumers and merchants include real-time funds transfer, irrevocability, and immediate settlement and funds availability.

Tokenization provides the bridge for these real-time payments to integrate with the connected vehicle infrastructure. The recent effort by leading financial institutions to develop a new digital wallet will challenge the dominance of existing wallets. This increased competition may spur the evolution of the digital wallet to become agnostic to payment type and channel.

2.4 Enrollment

Enrolling a payment method into a connected car is similar to the process used with other mobile wallets or applications that have payment capability. Vehicle manufacturers typically have a dealer delivery process for customers purchasing or leasing a new vehicle. The primary purpose of the process is to educate the customer and demonstrate key features and functionality. The salesperson is responsible for helping the customer load and activate their payment credential in the vehicle head unit and companion smartphone application. Alternatively, the consumer may need to use the car display to add, update, or remove their payment credentials from the in-car wallet if a used vehicle is being purchased, if the vehicle is sold or damaged beyond repair, or if the consumer wants to add an alternate payment instrument. Depending on the vehicle, enrollment and other changes could be done manually or with over-the-air Near Field Communication (NFC) provisioning.

2.5 Merchant Category Code (MCC)[2]

Another important consideration is the appropriate merchant category code used for the transaction. One reason is that issuers need to be able to properly identify transactions for rewards and other consumer benefits and correctly classify transactions to help avoid cardholder complaints.

Additionally, there are various authorization methods such as preauthorization, estimated, and incremental authorization that can benefit specific industries by using the appropriate MCC in the connected car space.

Merchants and their vendors should consult with their acquirers to access network documentation on the proper use of MCCs.

2.6 Payment Network Certification

The mobile payment provider application is a cloud-based application provided by the mobile payment processor (MPP) responsible for providing the interface between the token vault or token/trusted service provider, the mobile payment application, the site system, and the payment front-end processor (PFEP) in order to authorize transactions. The mobile provider should be certified with the provider for other payments (e.g., in-store) to make operations more seamless.

2.7 EMV® 3D Secure

EMV 3D Secure, or 3DS, is an authentication protocol used to enhance the security of online card transactions. 3DS supports an exchange of data, with information being shared between the merchant/car payment device enabling the issuer to make a risk-based decision resulting in either a frictionless transaction or a cardholder challenge. Friction can be minimized through a combination of provisioning with strong assurance (strong authentication), the use of payment tokens, the inclusion of critical data (e.g., device information, etc.), and/or participating in a Delegated Authentication program. It is recommended to refer to each payment network as the terms of their Delegated Authentication program may vary (e.g., a FIDO-certified biometric authenticator must be used, and the transaction must be tokenized).

[2] https://usa.visa.com/content/dam/VCOM/global/support-legal/documents/faqs-about-using-mcc-5552.pdf

Because car payments may be considered card-not-present transactions, there may be instances where the consumer needs to complete a first-time enrollment or authenticate the transaction. It is recommended that anyone considering connected cars and contextual payments become familiar with the global industry standard and each payment network's rules, requirements, and policies to determine any possible business impacts.

The following scenarios illustrate the potential impacts of 3DS.

Scenario 1 – Connectivity

A card has been successfully provisioned to the in-vehicle payment system.

The cardholder attempts to make a purchase with a merchant who supports 3DS. Challenge questions are sent to the cardholder, but the cardholder is unable to answer the challenge questions because of an unstable internet connection, which is more common in a moving car. The authentication process may fail or be delayed.

Scenario 2 – Safety

A card has been successfully provisioned to the in-vehicle payment system.

The cardholder attempts to make a purchase with a merchant who supports 3DS. Challenge questions are sent to the cardholder, but the cardholder is unable to answer the challenge questions because they cannot safely do so while they are operating a vehicle.

Scenario 3 – Shared Account Provisioning

A household member loads a 'shared account' card into the in-vehicle payment system. Challenge questions are sent to the primary cardholder either via text or email. The primary cardholder may be unaware that the household member is attempting to provision the card to the wallet, and may fail to answer the challenge questions, which then blocks the use of the card without further interaction with the primary account holder.

Scenario 4 – Shared Account Purchasing

A card has been successfully provisioned to the in-vehicle payment system.

A household member with the same primary account number (PAN) attempts to make a purchase with a merchant who supports 3DS. Challenge questions are sent to the primary account holder, who may be unaware of the attempted purchase and fail to answer the challenge questions, blocking the use of the card without further interaction with the primary account holder.

2.8 Wireless Reliability

Wireless connection reliability is crucial for connected car payment applications. Connected car payments often involve real-time transaction processing, where payment authorization and confirmation need to happen promptly. Unreliable wireless connectivity can result in transaction failures, declined payments, or delays in processing, leading to user frustration and potential disruptions in their experiences. While the reliability of the wireless infrastructure is typically out of the control of individual merchants, implementers of connected car applications should design their applications and processes to mitigate unreliable connectivity.

3. Security Considerations

Security stands as a paramount concern with payments and connected car technology. Sensitive financial information and personal data must be protected from potential threats and unauthorized access. Establishing robust security measures including the following, as applicable, can help to not only safeguard individuals' privacy but also maintain the trust essential for the widespread adoption of these technologies.

Governance and Compliance

- Follow regulatory or compliance standards, including PCI DSS, ISO 27001, ISO 15118, Security Operations Center (SOC), and privacy laws (including the California Consumer Privacy Act (CCPA) and other emerging privacy laws).
- For SOC, adhere to the five trust principles (availability, confidentiality, integrity, privacy, and security).
- Perform regular third-party audits, penetration tests, vulnerability assessments, and other tests and reviews for systems, personnel, and infrastructure.
- Establish data protection and security policies, procedures, and guidelines for employees, contractors, and other agents of the company, including privacy/security training, and system/data access rights with multifactor authentication (digital) or badge access (physical).
- Establish a cyber incident response plan, including the process and timeline for notices and applicable supervisory authority.
- Establish a disaster recovery and/or business continuity plan, including test plans.
- Establish secure coding practices (e.g., Open Worldwide Application Security Project [OWASP]) and web application security testing processes.

Data Access, Integration, and Storage

- For cloud-hosted systems and data storage, follow the Cloud Security Alliance standards.
- Encrypt data at rest using the AES-256 encryption standard and data in transit using TLS 1.2.
- Establish a data retention policy.
- Establish processes for account access, provisioning, and decommissioning, including third-party service providers and vendors.

Data Subject Rights

- Establish a data privacy notice policy that includes providing notices to consumers regarding collection, use, disclosure, and procedures to satisfy the data subject's right to access data. Define processes that manage requests in a timely manner.
- Establish procedures which satisfy data portability requests and deletion requests.

Implementers are advised to contact their security professionals to ensure that all applicable security, regulatory, and privacy standards are being followed.

4. Use Cases

Connected car use cases include (but are not limited to) the following examples:

Fueling

Consumers may authorize payment at a fuel dispenser and purchase add-on items (e.g., car washes), replicating the pay-at-pump experience from inside their vehicle. Implementations may include the use of data such as geolocation, pump states, and fuel prices to provide information to the consumer and ensure they are authorizing the intended fuel dispenser. This use case may extend to alternative fuels such as hydrogen and compressed natural gas.

Parking

Consumers may pay for parking from their cars. Implementations may include use of contextual data such as geolocation, parking sensors, and other data to direct consumers to available parking and handle payment.

Quick Service Restaurant (QSR) Order Ahead

Consumers may order food from their cars for pickup in store or from a drive-through lane. Implementations may include the use of contextual data such as geolocation, traffic conditions, and stored preferences to calculate pickup times and purchase totals including tip.

Queuing Mechanism for Services

The connected car may be placed in a queue for reservations (e.g., oil change, car wash) without requiring the car to physically queue. This implementation may include the use of geolocation and other contextual data for efficient queue management and use of a payment method to hold the reservation and provide prepayment.

Tolls

Instead of providing cash or electronic payment to an attendant or machine, the toll may be billed in the background based on a combination of geolocation, license plate scanning and, in the case of variable toll roads, dynamic pricing decisions.

In-Car Entertainment

For subscription services, payment is typically tied to a subscription identifier that is unique to the vehicle. Geolocation data may be used to influence available programming (e.g., sporting event blackout in an area).

Car On-Demand Features

Connected car subscription services may facilitate over-the-air software updates for the vehicle's systems and features. These updates may enhance functionality, introduce new features, improve security, and fix bugs or performance issues without needing physical visits to a dealership. Users may benefit from software enhancements and improvements delivered seamlessly to their connected cars.

Loyalty

A new customer can be enrolled, or an existing customer can be linked to a loyalty account using consumer information provided by the car.

EV Charging

Drivers may use a mobile app or dashboard infotainment app that identifies and locates charging stations and navigates and plans routes to them based on consumption. The app may be used to initiate the charging session either through wireless or RFID connectivity. For more information about EV Open Payments, please see the U.S. Payments Forum's EV Open Payments Working Committee resources.

EV Plug & Charge

EV Plug & Charge (based on ISO 15118 standards[3]) enables charging (AC and DC charging, plug & charge, smart charging) where the EV driver simply plugs the vehicle into the charge point. Using the ISO 15118 interface, the EV identifies itself to the charging station, allowing instant authorization and the initiation of charging. Plug & Charge currently requires a user account with the charge point operator but is currently expected to include payment tokenization in the near future to eliminate the need for an account with a charge point operator. Plug & Charge chargers require their own network connectivity like all EV chargers, but since a wireless connection for an app to communicate to the charger is not needed, chargers can be placed in environments such as underground parking garages, where an app may be limited due to poor wireless connectivity.

Smart Grid Interaction (Vehicle to Grid [V2G])

Under this use case, the EV communicates with the grid to schedule and perform intelligent charging based on the grid's load and/or can supply energy to the grid when supported.

[3] https://www.iso.org/standard/69113.html

5. Authentication

Authentication is the process of validating the identity of a registered user or process before enabling access to protected networks and systems. Authorization validates that an authenticated user or process has been granted permission to access the specific resource that has been requested. Identity management is the single most important component of any digital solution, and its operational and security integrity is critical. Authentication and identity management in the retail segment are generally tightly coupled to help minimize fraud and guarantee customer security. Identity management is the key operational and fraud control point; not having 100 percent visibility of the identity service can lead to outages, account takeover, costly fault-finding investigations, and latency in detecting and managing fraud. Careful consideration and implementation of the following will help support robust authorization and identity management in the connected car environment:

- Authentication requirements for connected car applications that include supporting and enabling marketplace applications, the underlying business relationships, and the user identity required to enable these partnerships.
- Authentication and identity management solutions that include multifactor authentication with consideration for PCI DSS, data protection regulations, and fraud prevention. Examples include using SMS as a second validation source, mobile phone number/account validation, and device-enabled biometrics.
- To support connected commerce applications enabled by third-party partnerships, authentication and identity management platforms that include support for different registration requirements, different verification/password reset standards and flows, different implementation of standards, and different security standards.
- An integrated approach to authentication, identity management, and security that is based on continuously predicting, detecting, learning, and protecting the user's identity in real time, making accurate decisions about new and emerging threats, and verifying authentic users. Related considerations include:
    - Device user verification. Properly identifying the device and user to reduce the risk of spoofed identity or fraudulent purchases.
    - CNP best practices. Performing real-time verification that a card is linked to a valid account and repeat verification when each new transaction is performed.
    - Behavioral analytics. Continuously verifying the user is behaving as expected.

In part, the broad success of contextual payments in the connected car environment will depend on the ability to bring integrated authentication solutions to the market that increase utility, while enabling digital collaboration, reducing customer friction, and supporting flexible solutions that overcome the following challenges:

- Varying registration requirements
- Varying verification/password reset standards
- Varying implementation of standards
- Varying interpretations of security standards

Additionally, strong industry collaboration may support implementation and user experience, including by helping to address the following complexities:

- Initial user onboarding complexities.
- Multiple logins and registrations to attach accounts.
- Many consumer accounts can be decades old with forgotten passwords and lost reset details. Data quality issues add to this complexity.
- Logouts that require the customer to re-login for each service.
- The need for customers to remember multiple passwords and account IDs.

As the number of devices and connected car services rise, new identity use cases, innovations, and authentication methods will need to be considered to enhance user experience without compromising security. Integrating everyday commerce into the vehicle through in-car wallets is one means of enabling users to pay for fuel, parking, EV charging, drive-through meals, or anything else from the comfort of their driver's seat.

6. Conclusion

In conclusion, the convergence of connected cars and contextual payments is poised to redefine mobility and commerce. As technology continues to advance, collaboration and innovation will shape the trajectory of this ecosystem. The possibilities are boundless. This white paper serves as a guiding resource for anyone seeking to understand, embrace, and capitalize on this exciting juncture of technology and finance.

7. Acknowledgements

This white paper was developed by the U.S. Payments Forum to provide analysis of the synergy between the connected car and contextual payments, explore real-world examples, and equip stakeholders across industries with the knowledge needed to navigate this evolving landscape successfully. Publication of this document by the U.S. Payments Forum does not imply the endorsement of any of the member organizations of the Forum.

The U.S. Payments Forum thanks **Nancy Kriens** of American Express and **Bradford Loewy** of NCR Voyix for leading this project, **Donald Frieden** of P97, **Eric Lim** of U.S. Bank, and **Tony Petit** of Visa, for drafting the white paper, and Working Committee members for their contributions. Participants involved in the project team developing and reviewing this white paper included:

Participants	
Nancy Kriens, American Express	**Donald Frieden, P97**
Robert McEntee, Cubic Transportation Systems	**Tony Petit, Visa**
Julius Alexander III, Discover Financial Services	**KJ Condie, Voyager (U.S. Bank)**
Nathan Markiecki, Discover Financial Services	**Eric Lim, U.S. Bank**
Bradford Loewy, NCR Voyix	

8. Legal Notice

This document is provided solely as a convenience to its readers, as an overview of considerations and use cases relating to contextual payments in the connected card environment. While great effort has been made to ensure that the information provided in this document is accurate and current, this document does not constitute legal or technical advice, should not be relied upon for any legal or technical purpose, and all warranties of any kind, whether express or implied, relating to this document, the information herein, or the use thereof are expressly disclaimed, including but not limited to warranties as to the accuracy, completeness or adequacy of such information, all implied warranties of merchantability and fitness for a particular purpose, and all warranties regarding title or non-infringement. Any person that uses or otherwise relies on the information set forth herein does so at his or her sole risk. This document provides only a high-level description of the subject matter and related considerations, and is not exhaustive; connected car and contextual payment implementations, circumstances and considerations may differ, as may corresponding stakeholder security and business needs, requirements, capabilities, and results, any of which may impact or be impacted by specific facts and circumstances. Accordingly, stakeholders interested in contextual payments and/or implementations in the connected car environment are strongly encouraged to consult with the relevant payment networks, acquirers, and other stakeholders, as well as appropriate subject matter experts and professional and legal advisors, prior to any implementation decisions.